Drivechain



- https://www.drivechain.info/
  - LayerTwo Labsの人？
- drivechain-project
- LayerTwo-Labs
- Grok
- ChatGPT, ChatGPT - CUSF
- 提案BIP
  - BIP-300(Hashrate Escrows)
  - BIP-301(Blind Merged Mining)
- その他
  - Drivechain Definition - CoinMarketCap
  - What's a Bitcoin Drivechain and Why Are Devs At Odds Over Its Proposal? - Decrypt

Bitcoin L1 を大きく変えずに、機能拡張をサイドチェーン(Drivechain sidechains)で実現しよう、という提案。

- サイドチェーン側で実験できる
- 失敗してもBitcoin本体には影響がない
- 双方向ペグで行き来できる
- Merged Mining でマイナーは普通にマイニングする手間で Drivechain もマイニングできる
  - 報酬がもらえるのでマイナーは参加してくれるはず
- Drivechain からの出金は3ヶ月かけて監視して Bitcoin本体に対して安全にする

BIP で提案しているのは、Federation に依存しない双方向ペグを Bitcoinプロトコルで安全にサポートする、というところだそうだ。

CUSF ChatGPT

Commitments to Unchained Soft Forks の略。

Bitcoinトランザクションにサイドチェーンの何かのハッシュ値をコミットメントとして埋め込み、オフチェーンで参照できるようにすること。 `OP_RETURN` などBitcoin自身には特に影響はさせないようにする。

Drivechain での用例としては、BIP-301 などの withdraw 提案の状態を記録したりしている。

(BIP-301 は CUSF とちょっと違うとかいってたんだけどね？)

Hashrate Escrows BIP-300(Hashrate Escrows)

サイドチェーンから Bitcoinへの出金を、マイナー投票と監視期間(3ヶ月)で承認するしくみ。

BTCのロック・解除ルールを Bitcoinプロトコルに組み込む

Federation無しの Two-way Peg をしたいなら(Drivechain以外の)どのチェーンでも利用できる

1. サイドチェーンの資金ロック
   Bitcoin L1上で特殊なエスクロー出力を作成し、そこに BTCをロックする
2. 入金(L1 → サイドチェーン)
   ユーザはBTCをそのエスクロー出力に送金
   サイドチェーン側はそれに対応するトークンを発行
3. 出金(サイドチェーン→L1)
   サイドチェーン上で burn して出金リクエストを作成
   あくまで「リクエスト」で
4. マイナー投票による承認
   不正防止のため、マイナーが複数ブロックに渡って投票
   投票期間は非常に長い(数ヶ月)。51%以上継続して指示された場合のみ承認される

peg-in した額以上は peg-out できないらしい。

じゃあ、サイドチェーン上で多く受け取ったらどうなるのだ？？

Merged Mining BIP-301(Blind Merged Mining)

マイナーがサイドチェーンブロックの内容を知らずにマイニングして報酬を得る。

1. サイドチェーン側のブロック作成者がブロックを作ってブロックハッシュ `h*` を作る
2. BMM Request というトランザクションを作り、この `h*` をcoinbaseトランザクションの `OP_RETURN` に入れてくれたら報酬を渡すよ、という情報を流す(BMM Requestトランザク

ション自体は報酬ではない。後払い)

3. BIP-301を処理できるマイナーがそのトランザクションを含み、coinbase トランザクションの `OP_RETURN` に BIP-301のフォーマットに従って `h*` を含めたブロックでマイニングする

4. マイニングが成功するとサイドチェーン側はそれを監視してブロックが承認されたと見なす

5. ブロック提案者はマイナーに報酬を払う

Bitcoin L1で行っているマイニングをサイドチェーン側のチェーンのマイニングに流用することでサイドチェーンのセキュリティを確保する。

Rootstock - Bitcoin L2でも使っているが方式が異なる。

Rootstock が merged mining + federated peg(中央的な署名者グループが存在する) なのに対して Drivechain は merged mining + miner-enforced peg(BIP-300/301によるマイナー投票) になっている。

Drivechain自体の特徴

- permissionless innovation
  - 許可なく新機能を実装可能
- 競合排除
  - 他プロジェクトのコードをBTCベースで取り込み、競争力強化

LayerTwo Labs

CEO は Paul Sztorc氏で Drivechainの提案者。2022年12月に300万ドルの資金調達ができている。

- Drivechainの開発と普及
- サイドチェーン設計
  - Ethereum や Zcash の機能とまったく同じものを含む複数のサイドチェーン設計を開発中
- ハイリスク・ハイリターンの問題への取り組み
  - 当たったら運営資金的に大きいよね、という意味のハイリスク・ハイリターン。
  - 予測市場（Prediction Markets）やNamecoin（ネームコイン）の復活など、通信やメディアに革新をもたらす可能性のある分野への取り組みも計画
    - Namecoin は 2011年にリリースされた Bitcoinからフォークしたアルトコイン
    - 分散型DNS
    - merged mining